

Towards Secure Authentication Standards for End-users, Industry and Academia

Nicolas Alexander Huaman Groschopf

In modern information security, user errors represent a major security risk, leading to a rise of phishing attacks, social engineering and impersonation that is used in many cybercrime attacks. However, blaming the user does not prevent these vulnerabilities. Instead, the area of usable security has started to focus on providing easy to understand and empowering interfaces and guidelines to support users. For this talk, I present results on the use of security measures in small and medium-sized enterprises. This work identifies password security as one of the major gaps in these enterprises. To address this, follow-up work looks at password managers as one approach to improve authentication security. One of my key findings is that standardization is missing for password managers. Alternative standards for authentication like FIDO2 and TOTP already exist, but currently do not succeed at replacing passwords. Therefore, I present final work covering interviews with 20 developers implementing and working with standards from the area of authentication, and its dependencies like cryptography. These interviews reveal key challenges like missing documentation for standards, as well as recommendations to improve standardization of security and authentication for developers and end-users alike. Traversing the full stack of stakeholders in secure authentication and communication, I conclude that there is a gap between the security research that is integrated into a standard and the usability research that only begins after the standardization process. I derive recommendations to improve authentication for stakeholders, be it end-users, industry, academia, or implementers of standards.